Public Works and Government Services Canada | Travaux publics et Services gouvernementaux Canada

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions - TPSGC
Place du Portage, Phase III
Core 0B2 / Noyau 0B2
11 Laurier St.\11, rue Laurier
Gatineau
K1A 0S5
Bid Fax: (819) 997-9776

SOLICITATION AMENDMENT
MODIFICATION DE L'INVITATION

The referenced document is hereby revised; unless otherwise indicated, all other terms and conditions of the Solicitation remain the same.

Ce document est par la présente révisé; sauf indication contraire, les modalités de l'invitation demeurent les mêmes.

Comments - Commentaires
THERE IS A SECURITY REQUIREMENT ASSOCIATED WITH THIS SOLICITATION

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Issuing Office - Bureau de distribution
Business Transformation and Systems Integration
Service/Division de transformation des opérations et d'intégrat
Special Procurement Initiative Dir
Dir. des initiatives speciales d'approvisionnement
11 Laurier, Place du Portage III
12C1
Gatineau
Québec
KIA 0S5

Title - Sujet ISS Transformation - RFP	
Solicitation No. - N° de l'invitation EP243-170549/B	**Amendment No. - N° modif.** 005
Client Reference No. - N° de référence du client 20170549	**Date** 2017-06-29
GETS Reference No. - N° de référence de SEAG PW-$$XE-678-31237	
File No. - N° de dossier 678xe.EP243-170549	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2017-08-11**	**Time Zone** **Fuseau horaire** Eastern Daylight Saving Time EDT
F.O.B. - F.A.B. **Plant-Usine:** ☐ **Destination:** ☑ **Other-Autre:** ☐	
Address Enquiries to: - Adresser toutes questions à: Oates, Christine	**Buyer Id - Id de l'acheteur** 678xe
Telephone No. - N° de téléphone (873) 469-3917 ( )	**FAX No. - N° de FAX** ( ) -
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:**	

Instructions: See Herein

Instructions: Voir aux présentes

Delivery Required - Livraison exigée	**Delivery Offered - Livraison proposée**
Vendor/Firm Name and Address **Raison sociale et adresse du fournisseur/de l'entrepreneur** **Telephone No. - N° de téléphone** **Facsimile No. - N° de télécopieur**	
Name and title of person authorized to sign on behalf of Vendor/Firm (type or print) **Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)** **Signature** **Date**	

Canada

Amendment Number 005

Purpose:

The purpose of this amendment is to extend the closing date of this Request for Proposal (RFP) and to provide answers to questions received with regards to this RFP.

A. QUESTIONS

Question 59:

Given the significance of the changes in Amendment 004, as well as the large number of outstanding answers to the questions submitted, it is requested that the closing date of the solicitation be extended by a period not less than 4 weeks.

Answer 59:

In consideration of recent changes and the outstanding responses to Bidder questions, Canada extends the closing date of the RFP to 2:00 PM (EDT) on August 11th, 2017.

Question 60:

We respectfully request an extension to July 28, 2017.

Answer 60:

Please see the response provided to Question 59 in this Amendment.

Question 61:

Has Canada developed a Business Needs for Security document that can be shared with Bidders?

Answer 61:

Yes. This document is provided in the current Amendment.

ALL OTHER TERMS AND CONDITIONS REMAIN THE SAME

Public Works and Government Services Canada
Travaux publics et Services gouvernementaux Canada

Canada

Respect ◆ Integrity ◆ Excellence ◆ Leadership

Serving GOVERNMENT, Serving CANADIANS.

Public Services and Procurement Canada

Industrial Security Program

BUSINESS NEEDS FOR SECURITY

Table of Contents

1. Introduction

1.1. Purpose

This document identifies the business needs for security of Industrial Security Program (ISP). It also identifies the security profile of the information system that will be implemented by the Industrial Security Systems Transformation Project (ISST) to support the ISP business activities.

1.2. Scope

This Business Needs for Security (BNS) assessment is applicable to the ISP business activities, which are comprised of business processes and their associated information assets.

1.3. Audience

This document is intended for:

- ISP program and service managers to understand the risks affecting the ISP, and the investment in IT security that is required to adequately manage these risks;
- Business and IT project managers, as well as IT and IT security practitioners as a primary source of guidance when architecting, engineering, designing, installing, and assessing the IT system(s) that support the ISP business activities;
- IT Security Directorate security analysts to assess the business needs for security of the ISP; and
- ISP business owner to authorize the use of IT system(s) that support ISP business activities.

1.4. Methodology

This BNS defines the security categorization of ISP business activities by analysing the program's business processes, information assets and threat agents that may affect them. In addition, the BNS ascertains the residual risk willing to be assumed by the ISP business owner after the application of security measures to the information system that will support the ISST project.

This BNS assessment is conducted in alignment with:

- The guidelines on IT security risk management that Communication Security Establishment (CSE) issued and maintain under Information Technology Security Guidance publication number 33 (ITSG-33) to help Government of Canada departments and agencies implement, operate and maintain dependable information systems;
- PSPC IT security processes and process assets; and
- Other Government and Industry IT risk management best practices.

2. Business Needs for Security

2.1. Business Context

The Industrial Security Program contributes to Canada's public safety and national security through its industrial security services by:

- Ensuring sensitive government assets and information, controlled goods and personnel are adequately safeguarded;
- Providing expertise to help counter the threats of espionage, weapons of mass destruction, and criminal and terrorist activities;
- Analyzing and investigating threats, while exchanging information with national and international partners;

The Industrial Security Program supports Canada's security agenda through the Contract Security Program and the Controlled Goods Program.

2.2. Applicable Legislation, Statues, and Regulations

This section outlines the regulatory environment of ISP. Legislation, statutes and regulations that affect the department as a whole are assumed applicable and therefore exclude from this section.

The following GC legislation as well as TBS and Departmental policy instruments are applicable to the Industrial Security Program:

a) Defence Production Act (DPA);
b) Controlled Goods Regulation (CGR);
c) Policy on Government Security (TBS-PGS);
d) Directive on Departmental Security Management (TBS-DDSM);
e) Standard on Security Screening (TBS-SSS);
f) Security and Contracting Management Standard (TBS-SCMS);
g) Security Organization and Administration Standard (TB-SOAS);
h) Operational Security Standard on Physical Security (TBS-PS);
i) Operational Security Standard: Management of Information Technology Security (TBS-MITS);
j) PSPC – DP 051: Departmental Security Program (PSPC-DSP);
k) PSPC - DP 054: Industrial Security Program (PSPC-ISP);
l) PSPC - DP 123: Policy on Compliance and Enforcement with Industrial Security Requirements (PSPC-PCEISR)
m) PSPC – DP 093: Policy on the Handling of Contract Security Incidents (PSPC-PHCSI)

2.3. Business Activities

This section describes ISP business activities which consist of the business processes and related information assets of the Industrial Security function.

Contract Security Program
The Contract Security Program (CSP) provides services that are vital to Canadians and the safeguarding of information and assets that are entrusted to Canadian and international private sector organizations and their governments. The program allows the GC to share both domestic and foreign sensitive technologies with the Canadian industry as well as allowing the Canadian industry the opportunity to participate in foreign classified

contracts. This program maintains the trust and confidence of NATO and other allies of Canada and supports the country's anti-proliferation, public safety, security and global security priorities.

CSP Business Activities:

1. CSP - Contracts Security: Ensures security in contracts awarded by PWGSC, or in contracts awarded by other government departments when requested;
2. CSP - Registration: Provides registration and security screening services to Canadian private sector organizations involved in protected/classified government contracts awarded by PWGSC or when registration and security screening services are requested by other government departments;
3. CSP - Personnel Security Screening: Evaluates the trustworthiness and loyalty of staff employed by private sector organizations participating in the CSP to Canada.
4. CSP - Requests for Visits: Processes Canadian and foreign visit requests for visitors requiring access to program or contract-related Classified / Protected information and assets;
5. CSP Documents Transfer: Facilitate the transmission of program or contract-related Classified/Protected information and assets between Canadian and foreign industries and governments; and
6. CSP - Investigations: Investigates reported cases of suspected contract security breaches.

Controlled Goods Program

The Controlled Goods Program (CGP) is a registration and compliance program which regulates access to controlled goods, including International Traffic in Arms Regulations (ITAR) items, in Canada. The CGP plays a vital role in the prevention and detection of the unlawful examination, possession or transfer of controlled goods in Canada. Under the authorities of the Defence Production Act (DPA) and the Controlled Goods Regulations, the CGP's mandate is to strengthen Canada's defence trade controls through the mandatory registration and regulation of businesses and individuals who examine, possess and/or transfer controlled goods.

CGP Business Activities:

7. CGP - Registration: Register individuals and organizations who examine, possess or transfer controlled goods in CGP;
8. CGP – Designated Officials Training and Certification: Provide training and certification services to Designated Officials (DO) of companies registered in CGP;
9. CGP - Exemptions: Exempt temporary workers, international students and visitors of companies registered in CGP from registration in the CGP;
10. CGP - Inspections and Compliance: Conduct inspections of sites where controlled goods are stored to ensure compliance with legal requirements;
11. CGP - Investigation and Analysis: Conduct security assessments of individuals and organizations that exceed the acceptable risk thresholds;
12. CGP - Case Management and Best Practices: Provides case management and investigative services in support of CGP;

The following table outlines the ISP business processes and associated information together with their authorities.

TABLE 1 – ISP BUSINESS ACTIVITIES

ID	Business Activity	Business Process	Component Description	Authoritative Source
1.1	CSP - Contracts Security	Pre-Contract Award	The *Contracts Security - Pre-Contract Award* business process evaluates the security requirements of procurement projects and provides security clauses to be included in the contracts solicitation documents.	Policy on Government Security (TBS-PGS); Directive on Departmental

ID	Business Activity	Business Process	Component Description	Authoritative Source
			The *Contracts Security - Pre-Contract Award* business process collects standard information related to projects security requirements. Data elements for Pre-Contract Award are described in TBS Security Requirements Check List (SRCL). The SRCL does not contain any information on prospective bidders or personal information. It simply documents the security requirements necessary for the applicable tenders or contracts.	Security Management (TBS-DDSM); Security and Contracting Management Standard (TBS-SCMS); Industrial Security Program (PSPC-ISP) Policy on Compliance and Enforcement with Industrial Security Requirements (PSPC-PCEISR)
1.2	CSP - Contracts Security	Post-Contract Award Review	The *Contracts Security - Post-Contract Award Review* business process reviews submitted contract information confirming compliance with the Policy on Government Security. The process also ensures that Government Protected and Classified contracts are afforded security consideration when amendments to the contracts are required or when the primary contract holder require work to be done by another organization. The *Contracts Security - Post-Contract Award Review* business process collects business and personal information, associated to government contracts. This includes SRCL, awarded contract and supplemental information, investigation results, inspections results, etc.	TBS-PGS; TBS-DDSM; TBS-SCMS; PSPC-ISP; PSPC-PCEISR Policy on the Handling of Contract Security Incidents (PSPC-PHCSI)
2.1	CSP - Registration	Registration in CSP	The *Registration in CSP* business process evaluates the eligibility of companies to access government contracts with security requirements and register or maintain their registration in CSP. Registration maintenance activities include updating registration information, as well as the upgrades, renewals and terminations of clearances. The *Registration in CSP* business process also verifies or initiate clearances with foreign partners to provide assurance that companies abroad meet the security requirements of GC contracts.	TBS-PGS; TBS-DDSM. TBS-SCMS; PSPC-ISP; PSPC-PCEISR; PSPC-PHCSI.

ID	Business Activity	Business Process	Component Description	Authoritative Source
			The *Registration in CSP* business process collects business and personal associated to Canadian Organizations that seek a new registration or wish to maintain existing a registration in CSP. Information elements include legal and business names, addresses, and telephone/fax numbers, personal details of Key Senior Officials, organization's parental and subsidiary information, security screening status, information about the contracts that have been awarded to the organization, etc.	
2.2	CSP - Registration	Registration in CSP-Organization Security Screening	The *Registration in CSP-Organization Security Screening* business process evaluates the eligibility of companies to work on government contracts with security requirements. Organizations that meet the contracts security requirements for Canadian and/or foreign government information/assets are granted their requested organizational security clearance, such as Designated Organizational Screening (DOS), Facility Safeguarding Capability (FSC), Document Safeguarding Capability (DSC), etc.	TBS-PGS; TBS-DDSM. TBS-SCMS; PSPC-ISP; PSPC-PCEISR; PSPC-PHCSI.
			The *Registration in CSP-Organization Security Screening* business process collects business and personal information related to the organizational structure, ownership, legal status, KSOs, Company Security Officer (CSO), details of facilities physical security safeguards (i.e., floor plans, location of motion sensor and or CCTV cameras, security cabinets, etc.), details of compliance with contracts IT security requirements, etc.	
3.1	CSP - Personnel Security Screening	Personnel Security Screening Requests	The *Personnel Security Screening Requests* business process evaluates the GC contractors' reliability and loyalty to Canada in order to grant and administer (i.e., update, upgrade, duplicate, transfer, reactivate, terminate, etc.) security clearances or site access clearances.	TBS-PGS; TBS-DDSM. TBS-SSS; PSPC-ISP;
			The *Personnel Security Screening Requests* business process requires the assessment of personal information including (but is not limited to): current and historical residence, financial status, family, education, employment, criminal convictions, out of country travel, legal status, military service, allegiances to Canada and/or states, etc.	

ID	Business Activity	Business Process	Component Description	Authoritative Source
3.2	CSP - Personnel Security Screening	Personnel Security Screening Investigations	The **Personnel Security Screening Investigations** business process assesses the government contractors' eligibility for security clearances when further information is required in order to address security concerns or to determine indoctrination for Top Secret SIGINT security clearances. The *Personnel Security Screening Investigations* business process collects and assesses sensitive personal information, such as the personnel`s criminal activity, association with radical or extremist groups, allegiance to foreign states, alcohol and/or illegal drug consumption, sexual conduct/behaviour, emotional or nervous disorders, military training, compulsive gambling, financial affluence or debts, details of foreign citizenships, etc.	TBS-PGS; TBS-DDSM. TBS-SSS; PSPC-ISP;
4.1	CSP - Requests for Visits	CSP Visits	The *CSP Visits* business process facilitates access to government sensitive information and/or assets to security-cleared individuals that visit a government or commercial organization in Canada or abroad, other than the site of the organization where they are employed. The *CSP Visits* business process (a.k.a. requests for visit) collects personal and business information associated to the visit. Data elements may include details of organizations and individuals security clearances, identification, information or assets to be accessed during the visit, etc.	TBS-PGS; TBS-DDSM; TBS-SCMS; PSPC-ISP; PSPC-PCEISR.
5.1	CSP Documents Transfer	Transfer of Sensitive Documents and Asset	The *Transfer of Sensitive Documents and Assets* business process ensures that information and assets that are transferred or exchanged as part of a sensitive government contract, whether in Canada or abroad, are safeguarded. The *Transfer of Sensitive Documents and Assets* business process collects personal and business associated to the stakeholders involved into the transfer of sensitive documents and assets.	TBS-PGS; TBS-DDSM; TBS-SCMS; PSPC-ISP; PSPC-PCEISR.
6.1	CSP - Investigations	Security Investigations	The Security Investigations business process facilitate administrative investigations when the confidentiality, integrity and/or availability of Government information or assets entrusted to private sector organizations have been compromised (lost or disclosed, modified or destroyed without authorization).	TBS-PGS; TBS-DDSM. TBS-SCMS; PSPC-ISP; PSPC-PCEISR;

ID	Business Activity	Business Process	Component Description	Authoritative Source
			The *Security Investigations* business process collects sensitive information related to contract security breaches involving the compromise of Government sensitive information or assets.	PSPC-PHCSI.
7.1	CGP - Registration	Registration in CGP - New Requests	The *Registration* in CGP-New Requests business process evaluates the eligibility of individuals and businesses to examine, possess or transfer controlled goods and register them in the CGP.	Defence Production Act (DPA)t; Controlled Goods Regulation (CGR);
			The *Registration* in CGP-New Requests business process collects personal and business information such as the business identification, legal status and ownership structure, the security assessment of Authorized Individuals and Designated Officials (current and historical information related to individuals identification, residence, financial status, family, education, employment, criminal convictions, out of country travel, legal status, military service, allegiances to Canada and/or states, etc.)	
8.1	CGP - DO Training and Certification	DO Training and Certification	The *CGP-Training and Certification business* process delivers training services to Designated Officials and certify them upon successful completion of the CGP exam.	DPA; CGR.
			The *CGP-Training and Certification business* process collects, store and process business and personal information associated to DOs that have participated in CGP training and certification. Examples of information elements include DOs identification, certification status, etc.	
9.1	CGP - Exemptions	Exemptions	The *Exemptions* business process evaluates the eligibility of Temporary Workers, International Students, or Visitors of an organization to be exempted from registration in the CGP but still be in contact with controlled goods.	DPA; CGR.
			The *Temporary Workers Exemptions* business process collects, process and store personal and business information such as individual's name, residence, date of birth, citizenship, description of controlled goods that the temporary worker or international student will examine, possess or transfer, etc.	

ID	Business Activity	Business Process	Component Description	Authoritative Source
10.1	CGP - Inspections and Compliance	CGP Inspections	The *CGP Inspection* business process evaluates security measures implemented by a CGP registrant to ensure that controlled goods are adequately safeguarded. The inspection also determines if examination, possession and transfer of controlled goods is conducted in compliance with legal requirements. The *CGP Inspection* business process collects, processes and stores information related to the assessed business compliance with legal requirements.	DPA; CGR.
11.1	CGP - Investigation and Analysis	CGP For Cause Referrals	The *CGP For Cause Referral* business process assesses high risks organizations and individuals in order to form a recommendation. For Cause Referrals are triggered by CGP registration or inspection business processes. The *CGP For Cause Referral* business process collects, process and store business and personal information such as the personnel`s criminal activity, association with radical or extremist groups, allegiance to foreign states, financial affluence or debts, details of foreign citizenships, etc.	DPA; CGR.
11.2	CGP - Investigation and Analysis	Industry Employee Referral	The *Industry Employee Referral* business process evaluates the eligibility of industry employees to examine or transfer controlled goods when a DO is unable to satisfactorily conclude the security assessment for an individual or if the assessed risk level is sufficiently high. The *Industry Employee Referral* business process collects, process and store personal information such as the personnel`s criminal activity, association with radical or extremist groups, allegiance to foreign states, financial affluence or debts, details of foreign citizenships, etc.	DPA; CGR.
12.1	CGP - Case Management and Best Practices	Case Management and Best Practices	The *Case Management and Best Practices* business process provides a detailed examination of problematic registration, inspection and visitor/temporary worker issues referred to it in order to make appropriate recommendations to concerned law enforcement, departments and agencies.	DPA; CGR.

ID	Business Activity	Business Process	Component Description	Authoritative Source
			The *Case Management and Best Practices* business process collect, store and process personal and business information such as the organization or personnel`s association with criminal activities, association with radical or extremist groups, allegiance to foreign states, financial affluence or debts, etc.	

2.4. Contractual Obligations

[…… Content Removed ……..][1]

2.5. Business Needs for Security

This section describes the business needs for security derived from the instruments identified in sections 2.2, 2.3 and 5.3.

Business Needs for Security is a fundamental element of the IT security risk management process. Statements of Business Needs for Security are used to influence the selection and tailoring of security controls, and serve to establish assurance that information systems implement these security controls in a way that fully satisfies legislative and regulatory requirements.

The Business Needs for Security summarized in *Table 2* are specific to ISP business activities and exclude general business needs for security identified by the PSPC in its Departmental BNS.

TABLE 2 – BUSINESS NEEDS FOR SECURITY BASED ON CONTRACTUAL OBLIGATIONS, LEGISLATION, STATUES, AND REGULATIONS

BNS-ID	Topic	Key Identified Business Needs for Security	Source
BNS-01	• Information Assurance; • Physical and IT security; • Security Incident Management; • Administrative investigations related to security incidents;	No person shall […] make any false or misleading statement or provide false or misleading information to an inspector or other person carrying out functions under this Act;	DPA S44
BNS-02	• Information Assurance; • Physical and IT security; • Security Incident Management; • Administrative investigations related to security incidents;	No person shall […] destroy any record or document required to be kept under this Act or the regulations;	DPA S44

[1] Note: The list of ISP agreements has been removed from this document version, for security reasons.

BNS-ID	Topic	Key Identified Business Needs for Security	Source
BNS-03	• Information Assurance; • Physical and IT security; • Security Incident Management; • Administrative investigations related to security incidents;	No person shall […] make a false entry in a record required to be kept under this Act or the regulations or omit to make any entry in such a record;	DPA S44
BNS-04	• Information Assurance; • Sharing information with other governments and organizations; • Obtaining Security services from other organizations; • Emergency and business continuity;	PSPC is identified as a lead security agency and mandated to "ensure the application of security safeguards through all phases of the contracting process within the scope of the Industrial Security Program"	TBS-PGS
BNS-05	• Information Assurance; • Physical and IT security; • Individual security screening; • Security in contracting; • Obtaining security services from other organizations; • Sharing information with other governments and organizations; • Protection of employees from workplace violence; • Security awareness and training; • Administrative investigations related to security incidents; • Emergency and business continuity;	The Assistant Deputy Minister, Departmental Oversight Branch, is responsible for administering the Industrial Security Program,	PSPC-DSP
BNS-06	• Information Assurance; • Physical and IT security; • Individual security screening; • Security in contracting; • Obtaining security services from other organizations; • Sharing information with other governments and organizations; • Protection of employees from workplace violence; • Security awareness and training; • Administrative investigations related to security incidents; • Emergency and business continuity;	"The Director, Canadian Industrial Security Directorate (CISD), Industrial Security Sector (ISS), is responsible for […] maintaining a database of private sector organizations and individuals that have been authorized to access classified and/or protected information and assets"	PSPC-ISP

BNS-ID	Topic	Key Identified Business Needs for Security	Source
BNS-07	• Information Assurance; • Physical and IT security; • Individual security screening; • Security in contracting; • Obtaining security services from other organizations; • Sharing information with other governments and organizations; • Protection of employees from workplace violence; • Security awareness and training; • Administrative investigations related to security incidents; • Emergency and business continuity;	"The Director, Controlled Goods Program, ISS, is responsible for […] maintaining a database of registered or exempt persons, with such database being available for consultation by registered private enterprises and public agencies"	PSPC-ISP
BNS-08	• Information Assurance; • Physical and IT security; • Individual security screening; • Security in contracting; • Obtaining security services from other organizations; • Sharing information with other governments and organizations; • Protection of employees from workplace violence; • Security awareness and training; • Administrative investigations related to security incidents; • Emergency and business continuity;	Security screening services are effective and efficient, and meet the needs of departments and agencies, and of the Government of Canada as a whole	TBS-SSS
BNS-09	• Information Assurance; • Physical and IT security; • Security in contracting; • Obtaining security services from other organizations; • Sharing information with other governments and organizations; • Security awareness and training; • Administrative investigations related to security incidents; • Emergency and business continuity;	The collection, use, disclosure, retention and disposal of personal information for the purpose of security screening is done in accordance with the *Privacy Act* and other applicable legislation, policies and directives;	TBS-SSS
BNS-10	• Information Assurance; • Individual security screening; • Security awareness and training;	[Executives and/or officials of organizations that are authorized to provide security screening services to departments and agencies are responsible for:]…. Ensuring that persons or organizations that are assigned responsibility for conducting security screening are qualified to do so and that they perform their responsibilities in accordance with legal, ethical and policy requirements, and with the security interests of Canada	TBS-SSS

BNS-ID	Topic	Key Identified Business Needs for Security	Source
BNS-11	• Information Assurance; • Physical and IT security; • Individual security screening; • Security in contracting; • Obtaining security services from other organizations; • Sharing information with other governments and organizations; • Protection of employees from workplace violence; • Security awareness and training; • Administrative investigations related to security incidents; Emergency and business continuity;	[Executives and/or officials of organizations that are authorized to provide security screening services to departments and agencies are responsible for:]…. Monitoring to ensure that the security screening services meet established service standards and that any issues relating to the fulfilment of service standards are investigated, acted on, and reported in a timely manner	TBS-SSS
BNS-12	• Information Assurance; • Physical and IT security; • Security in contracting; • Obtaining security services from other organizations; • Sharing information with other governments and organizations; • Security awareness and training; • Administrative investigations related to security incidents; • Emergency and business continuity;	Before any system to collect, process and manage personal information is put into operation, a risk assessment and a privacy impact assessment must be conducted, and security and privacy concerns must be mitigated to ensure that personal information is protected in accordance with the *Privacy Act* and related policy instruments.	TBS-SSS
BNS-13	• Information Assurance; • Physical and IT security; • Obtaining security services from other organizations; • Sharing information with other governments and organizations; • Administrative investigations related to security incidents; • Emergency and business continuity;	Individuals may also be required to provide other personal information to support the security screening process. That information may include vital events credentials (e.g., birth certificate, passport), biometrics (e.g., digital photographs, fingerprints), or letters of reference or referral	TBS-SSS
BNS-14	• Information Assurance; • Physical and IT security; • Security in contracting; • Obtaining security services from other organizations; • Sharing information with other governments and organizations; • Administrative investigations related to security incidents; • Emergency and business continuity;	In order for security screening to be conducted, individuals must provide their consent. By consenting, they authorize the indirect collection and the disclosure of information for security screening purposes. Until consent is obtained, information cannot be collected, used or disclosed.	TBS-SSS

BNS-ID	Topic	Key Identified Business Needs for Security	Source
BNS-15	• Information Assurance; • Physical and IT security; • Individual security screening; • Security in contracting; • Obtaining security services from other organizations; • Sharing information with other governments and organizations; • Administrative investigations related to security incidents; • Emergency and business continuity;	Personal information collected in security screening forms must be disclosed to security screening service providers both in government (e.g., the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP)) and outside government (e.g., credit bureaus) in order for the verifications, inquiries and assessments required for security screening to be conducted	TBS-SSS
BNS-16	• Information Assurance; • Physical and IT security; • Individual security screening; • Security in contracting; • Obtaining security services from other organizations; • Sharing information with other governments and organizations; • Administrative investigations related to security incidents; • Emergency and business continuity;	Personal information created, collected, used, disclosed, retained and disposed of for the purpose of security screening will be safeguarded in accordance with government standards for the protection of personal information, as well as the *Directive on Privacy Practices*. The level of categorization, and thereby protection, depends primarily on the sensitivity of the reports produced by CSIS or the RCMP.	TBS-SSS
BNS-17	• Information Assurance; • Physical and IT security; • Individual security screening; • Security in contracting; • Obtaining security services from other organizations; • Sharing information with other governments and organizations; • Administrative investigations related to security incidents; • Emergency and business continuity;	Access to, disclosure and handling of personal security screening information is to be monitored, documented, and limited to those who have a need to access it and who have a valid security status or clearance, using appropriate administrative, technical and physical security controls.	TBS-SSS
BNS-18	• Information Assurance; • Physical and IT security; • Individual security screening; • Security in contracting; • Obtaining security services from other organizations; • Sharing information with other governments and organizations; • Administrative investigations related to security incidents; • Emergency and business continuity;	Files will be created for each individual who undergoes security screening. These files contain relevant personal information, actions taken and decisions rendered in relation to the individual's security screening. Security screening service providers may also maintain records for **audit** purposes and for use when conducting security screening for updates or upgrades.	TBS-SSS

3. Threat Context

This section summarizes the threat context affecting the ISP business activities.

3.1. ISP Threat Environment

The ISP threat environment consists of:

a) The ISP operational environment (e.g., personnel, policies, business processes, information, information processing capacities, facilities, etc.);
b) The magnitude of natural/accidental threat events that may affect the ISP operations (e.g., earthquakes, pandemics, etc.); and
c) The capabilities (and motivation) of deliberate threat agents that may compromise the ISP operational environment.

All of these elements are interrelated and must be considered holistically in order to increase the ISP protection against threats.

3.2. Threat Categories affecting ISP

The main categories of threats affecting ISP business activities are grouped into Deliberate Threats and Natural/Accidental Threats. The two tables below indicate which categories of threats can affect the ISP business activities.

TABLE 3 - APPLICABLE DELIBERATE THREAT CATEGORIES

Threat Category	Threat Agent	Selected
Td1	Non-malicious adversary (e.g., non-malicious unauthorized browsing, modification, or destruction of information due to lack of training, concern, or attentiveness)	**Yes**
Td2	Passive, casual adversary with minimal resources who is willing to take little risk (e.g., listening, *script kiddie*)	**Yes**
Td3	Adversary with minimal resources who is willing to take significant risk (e.g., unsophisticated hackers)	**Yes**
Td4	Sophisticated adversary with moderate resources who is willing to take little risk (e.g., organized crime, sophisticated hackers, international corporations)	**Yes**
Td5	Sophisticated adversary with moderate resources who is willing to take significant risk (e.g., organized crime, international terrorists)	**Yes**
Td6	Extremely sophisticated adversary with abundant resources who is willing to take little risk (e.g., well-funded national laboratory, nation-state, international corporation)	**Yes**
Td7	Extremely sophisticated adversary with abundant resources who is willing to take extreme risk (e.g., nation-states in time of crisis)	**No**

TABLE 4- APPLICABLE NATURAL AND ACCIDENTAL THREAT CATEGORIES

Threat Category	Magnitude of Events	Selected
Ta1	• Minor accidental events (e.g., trip over a power cord, enter wrong information)	**Yes**
Ta2	• Moderate accidental events (e.g., render server inoperable, database corruption, release information to wrong individual or organization) • Minor hardware or software failures (e.g., hard disk failure) • Minor mechanical failures (e.g., power failure within a section of a facility) • Minor natural hazards (e.g., localized flooding, earthquake compromising part of a facility)	**Yes**
Ta3	• Serious inadvertent or accidental events (e.g., cut facility telecommunications or power cables, fire in a facility, large scale database corruption) • Moderate mechanical failures (e.g., long term facility power failure) • Moderate natural hazards (e.g., localized flooding or earthquake compromising a facility)	**Yes**
Ta4	• Serious mechanical failures (e.g., long term, city-wide power failure) • Serious natural hazards (e.g., earthquake with city-wide devastation)	**No**
Ta5	• Very serious mechanical failures (e.g., long term, regional power failure) • Very serious natural hazard (e.g., earthquake with regional or national devastation)	**No**

3.3. Description of the Threat Context

The threat profile of the ISP is expected to be **HIGH**.

[…… Content Removed ……..]

[2] Note: The analysis of ISP Threat Context has been removed from this document version, for security reasons.

4. Security Control Objectives

This section outlines the objectives of security controls to be selected, implemented, monitored, and maintained for ISP.

4.1. Information assurance

a) ISP Information must be protected from unauthorized access, use, disclosure, modification, disposal, transmission or destruction;
b) Access to ISP information must be limited to authorized individuals who have been security cleared and who have an express need for access;
c) Modification and destruction of ISP information must be limited to authorized individuals;
d) Appropriate security measures must be implemented for accessing, storing, transmitting and disposing of ISP information; and
e) The security of ISP information must be addressed through all phases of its life cycle or the life cycle of the information system to ensure security requirements are identified early, security controls are reviewed, management authorization is provided before operation and authorization is maintained through continuous monitoring of the security posture.

4.2. Individual security screening

a) All individuals who require access to ISP information, assets or facilities undergo an examination of their trustworthiness, honesty and, loyalty or reliability as it relates to loyalty to Canada before being granted access to ISP information, assets or sites.

4.3. Physical security

a) ISP Information, assets and facilities are protected from unauthorized access, disclosure, modification or destruction, in accordance with their level of sensitivity, criticality and value;
b) Access to ISP assets and facilities is limited to authorized individuals who have been security screened at the appropriate level and who have an express need for access;
c) Custodian-tenant relationships are defined in a formal agreement that ensures shared and individual responsibilities are addressed to achieve optimum security outcomes;
d) Security considerations are fully integrated into the process of planning, selecting, designing, modifying, building, implementing, operating and maintaining facilities and equipment;
e) External and internal environments of ISP facility are managed to create conditions that, together with specific physical security controls, reduce the risk of workplace violence, protect against unauthorized access, detect attempted or actual unauthorized access and activate an effective response; and
f) Containers, processes and procedures defined or recommended in GC standards and guidelines are used for the transport, transmittal, or destruction of ISP information and assets.

4.4. IT security

a) IT security considerations are fully integrated to meet business objectives at each stage of the IT system's life cycle, including definition, design, development, operations, maintenance and decommissioning;
b) Users must be identified and authenticated before access is granted to IT systems;
c) Access to ISP information and IT systems is limited to authorized users, including the types of transactions and functions that authorized users are permitted to exercise, based on business and security requirements;

d) Confidence in the security of IT systems is assured through the following:
   i) Assessing security controls;
   ii) Reducing or eliminating deficiencies;
   iii) Authorizing before operation; and
   iv) Maintaining authorization.
e) The IT security posture is continuously maintained by monitoring threats and vulnerabilities, detecting malicious activity and unauthorized access, and taking both pre-emptive and response actions to minimize effects;
f) IT system audit logs and records are created, protected and retained to enable monitoring, analysis and investigation so that users can be held accountable for their actions;
g) ISP data on all portable electronic media and devices are protected and sanitized or destroyed before disposal or reuse of the equipment; and
h) Electronic communications are protected by network security zones and perimeter defence at network boundaries;

4.5. Security in contracting

a) Security requirements are identified, addressed, formally documented, implemented and monitored in all phases of the procurement and throughout the life cycle of the contract; and
b) ISP information, assets, systems and facilities entrusted to industry meet the industrial security requirements and are afforded an appropriate level of protection throughout their life cycle.

4.6. Sharing information and assets with other governments and organizations

a) ISP information, assets and facilities entrusted to or shared with organizations outside the GC are afforded an appropriate level of protection throughout their life cycle;
b) Third-party information and assets entrusted to the ISP are afforded an appropriate level of protection throughout their life cycle; and
c) Documented arrangements clearly outline respective accountabilities and responsibilities of participants, in accordance with government and industry standards, and are periodically reviewed to confirm that they are still appropriate and relevant.

4.7. Obtaining security services from other organizations

a) Formal arrangements must be established when security services are obtained from another organization;
b) Arrangements contain security provisions that clearly outline respective accountabilities and responsibilities of the department and the service provider; and
c) Monitoring is conducted to verify compliance with security provisions, assess their continued relevance and update them as necessary.

4.8. Security awareness

a) A security awareness program covering all aspects of ISP and government security is established, managed, delivered and maintained to ensure that individuals having access to ISP information are informed and regularly reminded of security issues and concerns and of their security responsibilities; and
b) Individuals understand and comply with their security responsibilities and do not inadvertently compromise security.

4.9. Security training

a) Security practitioners and other individuals with specific security responsibilities receive appropriate and up-to-date training to ensure they have the necessary knowledge and competencies to effectively perform their security responsibilities and do not inadvertently compromise security.

4.10. Security incident management

a) Measures are taken to ensure preparedness and timely mitigation, response or recovery from security incidents and to prevent or minimize effects and potential losses;
b) Incidents that affect, or have the potential to affect, government-wide preparedness, mitigation, response or recovery from threats and vulnerabilities are reported to the appropriate lead security agency or law enforcement authority, and as appropriate, other departments when there is reason to believe that the security breach originated from that department; and
c) Post-incident analysis and follow-up is conducted and communicated to the appropriate lead security agency.

4.11. Protection of employees from workplace violence

a) Protective measures are in place to safeguard employees from workplace violence that could arise because of their duties or situations to which they may be exposed in the course of their work;
b) Information and training is available to employees regarding the handling of such situations; and
c) Thorough records and statements are maintained on reported incidents involving workplace violence.

4.12. Security inspections

a) Routine inspections are conducted of sites or systems where sensitive information and assets are processed or stored to ensure compliance with departmental security requirements (e.g., checking office areas during limited-access hours);
b) Security inspections are conducted in a manner that conforms to collective agreements and underlying legislation, are reasonable in the circumstances, and their procedures are made known to employees in advance of being performed;
c) Security inspections are conducted by assigned persons and do not target specific employees; and
d) Suspected violations or breaches of security are reported without delay and investigated as a basis for remedial action or reporting to the responsible authorities, as appropriate.

4.13. Administrative investigations related to security incidents

a) Investigations are conducted in a manner that does not jeopardize or compromise evidence, the rights of individuals or civil or criminal proceedings;
b) Procedures are developed and implemented to establish the conditions under which each administrative investigation will be conducted;
c) Incidents suspected of constituting criminal offences are reported to the appropriate law enforcement authority and protocols are established to ensure cooperation between the department and law enforcement agencies; and
d) Parties involved in the investigation are appropriately informed of their rights and obligations.

4.14. Security in emergency and increased threat situations

a) Plans and procedures are in place to escalate to heightened security levels in case of emergency and increased threat; and
b) ISP can coordinate with other emergency prevention and response plans (e.g., fire, bomb threats, hazardous materials, power failures, evacuations or civil emergencies) in the event of an emergency or increased threat situation.

4.15. Emergency and business continuity planning

a) Business continuity plans and contingency plans support the recovery and restoration of critical business services and functions and their associated assets and resources for uninterrupted minimum service delivery;
b) ISP services and assets are analyzed, identified and prioritized in terms of criticality;
c) An up-to-date inventory of critical services and associated information, assets and dependencies is maintained and provided to Department as requested;
d) Business continuity plans and recovery strategies are developed and arrangements made for all critical services; and
e) Business continuity plans are tested and readiness exercises conducted to ensure efficient and effective response and recovery.

5. Security Categorization

5.1. Injuries from Threat Compromise

The objective of injury assessment is to determine the expected injuries from threat compromise for each of the business processes and related information assets identified in Section 2.3. This is achieved by first determining the injuries that are likely to occur as a result of threats compromising the confidentiality, integrity, and availability of the business processes and related information assets, and then attributing appropriate levels of these injuries according to the departmental injury table (see Annex A).

The ISP collects store and process up to 35% of Protected B data, approximately 60% of Protected A data (the aggregate of which makes it Protected B as well) and less than 5% is Unclassified data.

The ISP also collects, store and process Secret and Protected C information, mainly in support of its investigative operations. This Secret and Protected C information accounts for less than 0.1% of the total volume of information collected, stored and processed by the ISP.

5.2. Injury Table

[…… Content Removed ……..][3]

[3] Note: The Injury Assessment Table has been removed from this document version, for security reasons.

5.3. Security Categorization of Business Activities

The security categorization of business activities is performed in order to ensure the selection and implementation of IT security controls for that the ISP Information System(s), These IT security controls must reflect the sensitivity and criticality of ISP business activities and information. A security category gives information system implementers, operators, and maintainers an appreciation of the importance of the business activities that their information systems support so that they can commensurately protect them.

The following tables provides a summary report on the injury assessment performed against the identified ISP business activities.

TABLE 6 –SECURITY CATEGORIZATION OF ISP BUSINESS ACTIVITIES

ID	Business Activity	Security Category		
		Confidentiality	Integrity	Availability
ISP Business Activities		**High**	**High**	**Medium**
1.1	CSP - Contracts Security Pre-Contract Award	[Content removed]	[Content removed]	[Content removed]
1.2	CSP - Contracts Security Post-Contract Award Review	[Content removed]	[Content removed]	[Content removed]
2.1	CSP - Registration Registration in CSP	[Content removed]	[Content removed]	[Content removed]
2.2	CSP - Registration Registration in CSP-Organization Security Screening	[Content removed]	[Content removed]	[Content removed]
3.1	CSP - Personnel Security Screening Personnel Security Screening Requests	[Content removed]	[Content removed]	[Content removed]
3.2	CSP - Personnel Security Screening Personnel Security Screening Investigations	[Content removed]	[Content removed]	[Content removed]
4.1	CSP - Requests for Visits CSP Visits	[Content removed]	[Content removed]	[Content removed]
5.1	CSP Documents Transfer Transfer of Sensitive Documents and Asset	[Content removed]	[Content removed]	[Content removed]
6.1	CSP – Investigations Security Investigations	[Content removed]	[Content removed]	[Content removed]
7.1	CGP – Registration Registration in CGP	[Content removed]	[Content removed]	[Content removed]

ID	Business Activity	Security Category		
		Confidentiality	Integrity	Availability
8.1	CGP - DO Training and Certification DO Training and Certification	[Content removed]	[Content removed]	[Content removed]
9.1	CGP - Exemptions Exemptions	[Content removed]	[Content removed]	[Content removed]
10.1	CGP - Inspections and Compliance CGP Inspections	[Content removed]	[Content removed]	[Content removed]
11.1	CGP - Investigation and Analysis CGP For Cause Referrals	[Content removed]	[Content removed]	[Content removed]
11.2	CGP - Investigation and Analysis Industry Employee Referral	[Content removed]	[Content removed]	[Content removed]
12.1	CGP - Case Management and Best Practices Case Management and Best Practices	[Content removed]	[Content removed]	[Content removed]

The security categorization of ISP business activities indicates a high watermark of **High** (High *Confidentiality / High Integrity / Medium Availability)*.

[……..Content Removed ……][4]

5.4. Security Profile of ISST Project

The current document provides a comprehensive description and categorization of the business needs for security for the ISP in its entirety. The scope of the ISST project is defined to exclude all Secret and Protected C information acquired, processed and stored by the ISP (comprising less than 0.1% of total ISP data by volume).

As a result, the security profile for the ISST project, while maintaining the High Integrity and Medium Availability requirement of the Program, bears a Medium Confidentiality requirement. The ISST project therefore requires the implementation of an information system with a security profile of *Medium Confidentiality / High Integrity / Medium Availability.*

[4] Note: The assessment of Security Categorization has been removed from this document version, for security reasons

6. Risk Tolerance

This section summarizes the acceptable residual risk for the Industrial Security Program.

ITSG-33 Annex 5, *Glossary* defines risk (IT security risk) as: "*the potential that a given threat will compromise IT assets and cause injury*", and the definition of residual risk as: "*A risk that remains after security controls have been selected, approved and implemented*." This degree of acceptability is typically expressed using acceptable residual risk levels on a qualitative scale from Very Low to Very High (per ITSG-33) or Low, Medium, High (per the GC Harmonized Threat and Risk Assessment Methodology).

Risk tolerance is defined as the "*The acceptable level of variation relative to achievement of a specific objective, and often is best measured in the same units as those used to measure the related objective".* In setting risk tolerance, management considers the relative importance of the related objective and aligns risk tolerances with organizational risk appetite and help to guide the organization's actions. Risk tolerance often is communicated in terms of acceptable residual risk.

By establishing acceptable residual risk levels, the ISP business owner assures the program key stakeholders of the degree of protection that they expect from the ISP IT systems.

The ISP has limited tolerance to risk and is willing to accept a Low residual risk for the IT system that will be implemented by the ISST project.

A Low risk tolerance level means that ISP is ready to assume low risks such as: minor inconveniences or minor financial loss that has no impact on ISP clients and partners. Safeguarding ISP business processes and information against such low vulnerabilities would not be worth the loss associated with it. This means that any residual risks deemed to have a medium to high impact are unacceptable.

7. Security Assurance and Robustness Level

This section defines the level of security assurance and robustness required for the Information System(s) that that support the ISP operations.

A security assurance level (SAL) consists of a pre-selected set of security assurance requirements that yields an incremental degree of confidence in the adequacy of the security engineering and documentation work to be performed by the project teams, and ultimately that the implemented security controls perform as intended and satisfy the ISP business needs for security.

The ISP requires for the information system that will be implemented by the ISST project a security assurance level of SAL-4.

A robustness level is an indication of the strength of security mechanisms that must be selected to satisfy security controls and security assurance efforts required for an Information System.

The ISP requires a robustness level of R4 for the information system that will be implemented by the ISST project to support ISP business activities

A robustness level of R4 requires strong, more costly security solutions, and imposes on IT projects a rigorous system security engineering process that exceeds the level at which they typically perform.

Annex A – Departmental Injury Table

Injury Type	Qualifier and Level				
	Very Low	Low	Medium	High	Very High
Civil disorder or unrest	No reasonable or negligible expectation of injury	Civil disobedience, public obstructions	Riot	Sabotage affecting critical assets (e.g., critical infrastructure)	Large scale riot or sabotage requiring martial law
Physical harm to people	No reasonable or negligible expectation of injury	Physical discomfort	Physical pain, injury, trauma, hardship, illness	Physical disability, loss of life	Widespread loss of life
Psychological harm to people	No reasonable or negligible expectation of injury	Stress	Distress, psychological trauma	Causing a mental disorder or illness	Widespread psychological trauma
Financial loss to individuals	No reasonable or negligible expectation of injury	Causing stress or discomfort	Affecting quality of life	Financial security compromised	N/A
Financial loss to Canadian companies	No reasonable or negligible expectation of injury	Affecting performance	Reducing competitiveness	Viability compromised	N/A
Financial loss to the Canadian government	No reasonable or negligible expectation of injury	Affecting program performance	Affecting program outcomes	Program viability compromised	Key programs viability compromised
Harm to Canadian economy	N/A	N/A	Affecting performance	Reducing international competitiveness	Compromising key economic sectors
Harm to Canada's reputation	No reasonable or negligible expectation of injury	Loss of Canadian public confidence	Embarrassment (home or abroad)	Damage to federal-provincial relations	Damage to diplomatic or international relations
Loss of Canadian sovereignty	N/A	N/A	Impediment to the development of major government policies	Impediments to effective law enforcement	

Annex B – References

Acts and Regulations

Financial Administration Act	http://laws-lois.justice.gc.ca/eng/acts/f-11/
Access to Information Act	http://laws-lois.justice.gc.ca/eng/acts/a-1/
Privacy Act	http://laws-lois.justice.gc.ca/eng/acts/p-21/
Personal Information Protection and Electronic Documents Act (PIPEDA)	http://laws-lois.justice.gc.ca/eng/acts/p-8.6/
Library and Archives of Canada Act	http://laws-lois.justice.gc.ca/eng/acts/l-7.7/
Official Languages Act	http://laws-lois.justice.gc.ca/eng/acts/o-3.01/
Defence Production Act	http://laws-lois.justice.gc.ca/eng/acts/d-1/
Visiting Forces Act	http://lois-laws.justice.gc.ca/eng/acts/V-2/
Criminal Code	http://laws-lois.justice.gc.ca/eng/acts/c-46/
Canada Evidence Act	http://laws-lois.justice.gc.ca/eng/acts/C-5/
Criminal Records Act	http://laws-lois.justice.gc.ca/eng/acts/c-47/
Export and Import Permits Act	http://laws-lois.justice.gc.ca/eng/acts/e-19/
Controlled Goods Regulation	http://laws-lois.justice.gc.ca/eng/regulations/SOR-2001-32/
Secure Electronic Signature Regulations	http://laws-lois.justice.gc.ca/eng/regulations/SOR-2005-30/page-1.html

Policies, Directives, Standards and Guidelines

Policy Framework for Information and Technology	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12452
Policy on Information Management	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12742
Policy on Management of Information Technology	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12755
Policy on Privacy Protection	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510
Policy on Access to Information	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12453
Policy on Government Security	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578
Directive on Departmental Security Management	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16579
Operational Security Standard: Management of Information Technology Security (MITS)	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328
Operational Security Standard on Physical Security	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12329
Standard on Security Screening	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28115
Security and Contracting Management Standard	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12332
Operational Standard for the Security of Information Act	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12323
Security Organization and Administration Standard	http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12333
Policy on Financial Management Governance	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=14005
Policy on Internal Audit	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16484
Policy on Communications and Federal Identity	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30683

Federal Identity Program Policy	ww.tbs-sct.gc.ca/hgw-cgf/oversight-surveillance/communications/fip-pcim/index-eng.asp
Directive on Identity Management	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16577
Directive on the Administration of the Access to Information Act	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18310
Directive on Management of Information Technology	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=15249
Policy on Acceptable Network and Device Use	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=27122

IT Security Guidelines

ITSG-33 IT Security Risk Management: A Lifecycle Approach	https://www.cse-cst.gc.ca/en/node/265/html/22814
ITSG-41 Security Requirements for Wireless Local Area Networks	https://www.cse-cst.gc.ca/en/node/264/html/15287
ITSG-38 Network Security Zoning - Design Considerations for Placement of Services within Zones	https://www.cse-cst.gc.ca/en/node/266/html/25034
ITSG-04 Threat and Risk Assessment Working Guide has been replaced by the Harmonized Threat and Risk Assessment Methodology (TRA)	https://www.cse-cst.gc.ca/en/publication/tra-1
ITSG-31 User Authentication Guidance for IT Systems	https://www.cse-cst.gc.ca/en/node/267/html/22784
ITSG-22 Baseline Security Requirements for Network Security Zones in the Government of Canada	https://www.cse-cst.gc.ca/en/node/268/html/15236
ITSP.30.031 V2 User Authentication Guidance for Information Technology Systems	https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsp.30.031v2-eng.pdf
Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information	https://www.cse-cst.gc.ca/en/node/1831/html/26515
User Authentication Guidance for Information Technology Systems	https://www.cse-cst.gc.ca/en/node/1842/html/26717
Clearing and Declassifying Electronic Data Storage Devices	https://www.cse-cst.gc.ca/en/publication/itsg-06
NIST SPECIAL PUBLICATIONS (SP)	http://csrc.nist.gov/publications/PubsSPs.html#SP 800

Contract Security Program - Forms and Guidelines

Industrial Security Manual	
Industrial Security Manual	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/index-eng.html
Personnel Security Screening	
Personnel Screening, Consent and Authorization form (TBS/SCT 330-23E)	http://www.tbs-sct.gc.ca/tbsf-fsct/330-23-eng.asp
Security Clearance form (TBS/SCT 330-60E)	http://www.tbs-sct.gc.ca/tbsf-fsct/330-60-eng.asp
Security Screening Certificate and Briefing form (TBS/SCT 330-47)	http://www.tbs-sct.gc.ca/tbsf-fsct/330-47-eng.asp

Security Requirements Check List (TBS/SCT 350-103)	http://www.tbs-sct.gc.ca/tbsf-fsct/350-103-eng.asp
Company security officer and alternate company security officer security incident report	http://iss-ssi.pwgsc-tpsgc.gc.ca/formulaires-forms/rapport-incident-report-eng.html
Company security officer or alternate company security officer attestation form	http://iss-ssi.pwgsc-tpsgc.gc.ca/formulaires-forms/attestation-eng.html
Consent to release of reliability screening and/or security clearance information	http://iss-ssi.pwgsc-tpsgc.gc.ca/formulaires-forms/cnsntmnt-cnsnt-eng.html
Personnel security screening forms tips	http://iss-ssi.pwgsc-tpsgc.gc.ca/formulaires-forms/conseils-tips-eng.html
Personnel security clearance form checklists	http://iss-ssi.pwgsc-tpsgc.gc.ca/formulaires-forms/liste-checklist-eng.html
Personnel security clearance form most common mistakes	http://iss-ssi.pwgsc-tpsgc.gc.ca/formulaires-forms/erreurs-mistakes-eng.html
Contract Security	
Security Requirements Check List (TBS/SCT 350-103)	http://www.tbs-sct.gc.ca/tbsf-fsct/350-103-eng.asp
Organization Security Screening	
Request for Private Sector Organization Screening form	http://iss-ssi.pwgsc-tpsgc.gc.ca/formulaires-forms/esosp-psos-eng.html
Annex 1-A – Corporate company security officer / company security officer security appointment and acknowledgement and undertaking	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-1a-eng.html
Annex 1-B – Alternate company security officer security appointment and acknowledgement and undertaking	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-1b-eng.html
Annex 3-G – Public Works and Government Services Canada – Security agreement	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-3g-eng.html
Annex 3-D – Resolution for the exemption of parent organization	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-3d-eng.html
Annex 3-E – Non-Disclosure certificate	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-3e-eng.html
Annex 3-F – Subsidiary board resolution noting parent's exclusion and resolution to exclude parent organization	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-3f-eng.html
How to complete a Request for Private Sector Organization Screening form	http://iss-ssi.pwgsc-tpsgc.gc.ca/formulaires-forms/esosp-psos-instructions-eng.html
Organization Safeguarding	
Annex 5-A – Registering document for equipment purchase	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-5a-eng.html
Transport and transmittal	
Appendix A-1 to annex 5-D – Courier certificate/itinerary	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-5d-app-a1-eng.html
Appendix A-3 to annex 5-D – Pre-trip declaration	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-5d-app-a3-eng.html
Appendix A-3 to annex 5-D – Pre-trip declaration	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-5d-app-a3-eng.html
Appendix A-4 to annex 5-D – Post-trip declaration	http://iss-ssi.pwgsc-tpsgc.gc.ca/msi-ism/anx-5d-app-a4-eng.html

Guideline for suggested transportation plan content	http://iss-ssi.pwgsc-tpsgc.gc.ca/formulaires-forms/pt-tp-eng.html
Guideline for suggested notice of classified consignment	http://iss-ssi.pwgsc-tpsgc.gc.ca/formulaires-forms/avis-notice-eng.html
Visits	
Request for visit (Domestic and International)	http://iss-ssi.pwgsc-tpsgc.gc.ca/formulaires-forms/visite-visits-eng.html
Instructions for completing the domestic request for visit form	http://iss-ssi.pwgsc-tpsgc.gc.ca/formulaires-forms/domestique-domestic-eng.html
Instructions for completing the international request for visit form	http://iss-ssi.pwgsc-tpsgc.gc.ca/formulaires-forms/internationale-international-eng.html

Controlled Goods Program - Forms and Guidelines

Registration	
Application for registration	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/ft-fo/inscription-registration-eng.html
Security assessment application - owner, authorized individual, designated official, officer, director, employee	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/ft-fo/des-saa-eng.html
Security assessment summary by designated official conducting a security assessment of an employee, director or officer	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/ft-fo/ses-sas-eng.html
Guideline on Controlled Goods Program registration	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/directives-guidelines/inscription-registration-eng.html
Guide to the New Schedule to the Defence Production Act	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/directives-guidelines/lpd-dpa-toc-eng.html
Inspections and Compliance	
Guideline on Controlled Goods Program compliance inspections	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/directives-guidelines/inspections-eng.html
Pre-inspection self-assessment checklist	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/ressources-resources/publications/pre-inspection-eng.html
Security breach report form	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/ft-fo/as-sbr-eng.html
Registration Exemptions	
Application for exemption for registration—temporary worker/international student	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/ft-fo/travailleur-worker-eng.html
Visitor application for security assessment and exemption from registration form	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/ft-fo/visiteurs-visitors-eng.html
Security assessment application—temporary worker/international student	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/ft-fo/des-travailleur-saa-worker-eng.html
Designated Officials	
Designated Official Certification Program	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/formation-training-eng.html
Guideline for Designated Officials	http://iss-ssi.pwgsc-tpsgc.gc.ca/dmc-cgd/directives-guidelines/rd-directives-do-guidelines-eng.html